

THIS PAGE BLANK (USPTO)

①-⑨/9

P3014

(19) 日本国特許庁 (JP)

再公表特許(A1)

(11) 国際公開番号

WO2003/071753

発行日 平成17年6月16日 (2005. 6. 16)

(43) 国際公開日 平成15年8月28日 (2003. 8. 28)

(51) Int. Cl. ⁷

F 1

H 0 4 L 12/58

H 0 4 L 12/58

1 0 0 F

G 0 6 F 13/00

G 0 6 F 13/00

6 1 0 Q

審査請求 未請求 予備審査請求 有 (全 23 頁)

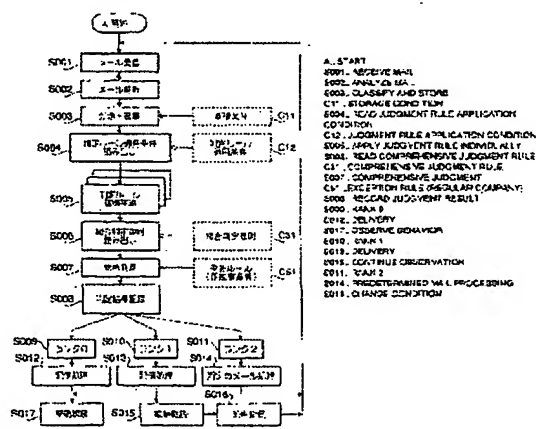
出願番号 特願2003-570531 (P2003-570531)
 (21) 国際出願番号 PCT/JP2003/001831
 (22) 国際出願日 平成15年2月19日 (2003. 2. 19)
 (31) 優先権主張番号 特願2002-46049 (P2002-46049)
 (32) 優先日 平成14年2月22日 (2002. 2. 22)
 (33) 優先権主張国 日本国 (JP)
 (81) 指定国 AP (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), EA (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OA (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, B, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, M, X, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(71) 出願人 591112522
 株式会社アクセス
 東京都千代田区猿樂町二丁目8番16号
 (74) 代理人 100078880
 弁理士 松岡 修平
 (72) 発明者 山上 俊彦
 東京都千代田区猿樂町二丁目8番16号
 株式会社アクセス内

(54) 【発明の名称】 利用者にとって好ましくない電子メールを処理するための方法および装置

(57) 【要約】

電子メール受信すると共に、受信した電子メールを、ヘッダ部に含まれる中継経路情報に基づいて分類して蓄積する。各分類に対して、少なくとも (1) 単位時間当たりの受信数が第1所定値以上である、(2) 宛先アドレスが有効でないメール数が第2所定値以上である、を含む判定ルールによる判定を行う。そして、成立する判定規則の項目の数が所定数以上であった分類の電子メールについては、(a) 利用者への配信をブロックする、(b) 発信元へ、不達メールを擬似的に再現した疑似エラーメッセージを送信する、というメール処理を行う。



【特許請求の範囲】**【請求項 1】**

利用者にとって好ましくない所定の種類の電子メールを選び出して処理するための方法であって、

発信元から利用者に至るまでの経路の途中で電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、受信した前記電子メールを分類して蓄積し、

前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定すること、を特徴とする電子メール処理方法。

【請求項 2】

前記所定の情報は、同一の発信元から送信された蓋然性の高い電子メールの一群を特定するための情報であること、を特徴とする請求項 1 に記載の電子メール処理方法。

【請求項 3】

前記同一の発信元から送信された蓋然性の高い電子メールの一群を特定するための情報は、前記電子メールの中継に関する情報であること、を特徴とする請求項 2 に記載の電子メール処理方法。

【請求項 4】

前記中継に関する情報は、中継経路の情報であり、前記分類は該中継経路毎に行われること、を特徴とする請求項 3 に記載の電子メール処理方法。

【請求項 5】

前記中継に関する情報は、中継経路中にある中継機のサーバ名またはドメイン名であり、前記分類は、該サーバ名またはドメイン名毎に行われること、を特徴とする請求項 3 に記載の電子メール処理方法。

【請求項 6】

前記所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定することは、前記所定の種類の電子メールであるか否かについてランク付けすることを含む、請求項 1 に記載の電子メール処理方法。

【請求項 7】

前記ランク付けによるランクに応じて、前記各分類の電子メールに対して異なる処理を実行することをさらに含むこと、を特徴とする請求項 6 に記載の電子メール処理方法。

【請求項 8】

前記所定のアルゴリズムによって、前記各分類の電子メールを、前記所定の種類の電子メールであるもの、前記所定の種類の電子メールの可能性のあるもの、通常の電子メールの少なくとも 3 つのランクにランク付けすること、を特徴とする請求項 6 に記載の電子メール処理方法。

【請求項 9】

前記ランク付けの段階数は可変であること、を特徴とする請求項 6 に記載の電子メール処理方法。

【請求項 10】

前記所定のアルゴリズムは、前記各分類の電子メールに対して前記ランク付けを行うための基準として用いる、それぞれのランクに対応したしきい値を含むと共に、該しきい値の値は可変であること、を特徴とする請求項 6 に記載の電子メール処理方法。

【請求項 11】

前記所定のアルゴリズムが変更可能であること、を特徴とする請求項 1 に記載の電子メール処理方法。

【請求項 12】

前記所定のアルゴリズムは、前記分類して蓄積された電子メールに関して、それぞれの分類毎に、下記項目、

(1) 単位時間当たりの受信数が第 1 所定値以上である

(2) 宛先アドレスが有効でないメール数が第 2 所定値以上である

のうち 1 つ以上を含む判定規則について前記判定規則の各項目が成立するか否かを判定することを含み、

前記判定の結果に基づいて前記各分類の電子メールが前記所定の種類の電子メールであるか否かを判定すること、を特徴とする請求項 1 に記載の電子メール処理

方法。

【請求項 1 3】

前記所定のアルゴリズムは、前記分類して蓄積された電子メールに関して、それぞれの分類毎に、下記の判定規則、

- (1) 単位時間当たりの受信数が第 1 所定値以上である
- (2) 宛先アドレスが有効でないメール数が第 2 所定値以上である
- (3) 発信元アドレスが無効である
- (4) 分類内の電子メールの宛先アドレスの相違の度合いが第 3 所定値以上である
- (5) メール本文中に所定の内容が含まれる
- (6) メール本文中に所定の URL が含まれる

のうち少なくとも 1 つについて成立するか否かを判定することを含み、前記判定の結果に基づいて前記各分類の電子メールが前記所定の種類の電子メールであるか否かを判定すること、を特徴とする請求項 1 に記載の電子メール処理方法。

【請求項 1 4】

前記判定規則 (4) の宛先アドレスの相違の度合いは、各宛先アドレスの符号の間のハミング距離に基づいて算出されること、を特徴とする請求項 1 3 に記載の電子メール処理方法。

【請求項 1 5】

前記電子メールを受信して分類し蓄積することを、蓄積時間、蓄積メール数の少なくとも一方を定めた蓄積条件に達するまで行うことをさらに含むこと、を特徴とする請求項 1 に記載の電子メール処理方法。

【請求項 1 6】

前記判定の結果、前記所定の種類の電子メールと判定された電子メールについて、該判定された電子メールの送信先の利用者の情報が前記所定の種類の電子メールの発信元に送信されることを防止する処理を行うことをさらに含むこと、を特徴とする請求項 1 に記載の電子メール処理方法。

【請求項 1 7】

前記判定の結果、前記所定の種類の電子メールと判定された電子メールについて

- (a) 利用者への配信をブロックする
 - (b) 発信元へ、不達の場合にメールサーバが発信元に対して送り返す不達メールを擬似的に再現した疑似エラーメッセージを送信する
 - (c) 消去する
 - (d) 所定のメールサーバから不達メールが発信される場合に、当該不達メールが発信元に返信されるのを抑止する
 - (e) 発信元に対して警告メッセージを送信する
 - (f) 当該分類の電子メールに関する情報を保存しておく
 - (g) 利用者に対し当該分類の電子メールを配信すべきか否かの問い合わせを行い、該問い合わせに対する利用者からの応答に応じて処理を行う
 - (h) 当該分類の発信元に対応する装置に対しては、所定のメールサーバについてのドメインネームサービスが拒否されるようにする
 - (i) 当該分類の発信元に対応する装置のIPアドレスに対しては、所定のメールサーバに対する接続の要求が拒否されるようにする
- のうち少なくとも1つを含む処理を行うことをさらに含むこと、を特徴とする請求項1に記載の電子メール処理方法。

【請求項18】

前記電子メールは、送信先の利用者への電子メールが不達であった場合に、所定のメールサーバから発信元に転送される不達メールを含むこと、を特徴とする請求項1に記載の電子メール処理方法。

【請求項19】

電子メールを受信すると共に、該受信した電子メールに含まれる発信元および／またはメールの中継に関する情報に基づいて、前記受信した電子メールを分類して蓄積し、

前記電子メールを受信して分類し蓄積することを、蓄積時間、蓄積メール数の少なくとも一方を定めた蓄積条件に達するまで行い、

下記の項目(1)から(6)、

- (1) 単位時間当たりの受信数が第1所定値以上である
- (2) 宛先アドレスが有効でないメール数が第2所定値以上である
- (3) 発信元アドレスが無効である
- (4) 分類内の電子メールの宛先アドレスの相違の度合いが第3所定値以上である
- (5) メール本文中に所定の内容が含まれる
- (6) メール本文中に所定のURLが含まれる

のうち1つ以上を含む判定規則に関して前記判定規則に含まれる項目のうちどの項目を適用するかを指定した判定規則適用条件に基づいて、前記分類して蓄積された電子メールについて、前記それぞれの分類毎に、前記判定規則適用条件で指定された各項目が成立するか否かを判定し、

前記判定規則適用条件で指定された項目のうち、成立する項目の数を判定成立の条件として用いる総合判定規則にしたがって、前記それぞれの分類毎に、前記総合判定規則が成立するかどうかの判定を行い、

前記総合判定規則が成立すると判定された分類の電子メールについて、

- (a) 利用者への配信をブロックする
- (b) 発信元へ、不達の場合にメールサーバが発信元に対して送り返す不達メールを擬似的に再現した疑似エラーメッセージを送信する

のうち少なくとも1つを含む所定のメール処理を実行すること、を特徴とする電子メール処理方法。

【請求項20】

請求項19に記載の電子メール処理方法において、さらに、

前記電子メール処理方法に記載の一連の処理を少なくとも1回以上実行することによって、前記総合判定規則の判定結果に関する統計的な値を取得し、

取得された前記統計的な値に応じて、前記蓄積条件、前記判定規則、前記判定規則適用条件、前記総合判定規則のうち少なくともいずれか1つについて内容の設定または変更を行うこと、を特徴とする電子メール処理方法。

【請求項21】

請求項19に記載の電子メール処理方法において、さらに、

前記蓄積条件、前記判定規則、前記判定規則適用条件、前記総合判定規則のうち少なくともいずれか1つについて、ユーザインタフェースを介して内容の設定または変更を受け付けること、を特徴とする電子メール処理方法。

【請求項22】

請求項19に記載の電子メール処理方法において、さらに、
前記総合判定規則が成立した場合でも、所定の例外規則に該当する分類については前記所定のメール処理の対象とはしないこと、を特徴とする電子メール処理方法。

【請求項23】

請求項22に記載の電子メール処理方法において、
前記所定の例外規則は、例外とすべき発信元のアドレス、例外とすべき発信元のドメイン名、前記所定のメール処理を実行しない時間帯、前記所定のメール処理を実行しない期間の少なくともいずれか一つを含むこと、を特徴とする電子メール処理方法。

【請求項24】

請求項19に記載の電子メール処理方法において、さらに、
利用者が所定のメールサーバに対して、ドメイン名、発信元アドレスの少なくとも1つを含む、電子メールの配信を希望しない配信拒否条件の登録をしている場合に、前記所定のメールサーバから前記配信拒否条件を取得し、
取得した前記配信拒否条件に基づいて前記所定のメール処理の対象とする分類を決定すること、を特徴とする電子メール処理方法。

【請求項25】

請求項19に記載の電子メール処理方法において、
前記総合判定規則には、前記判定規則適用条件で指定された判定規則の項目のうち、成立する判定規則の項目の数がランク付けの要因として定められ、
総合判定規則にしたがって、前記それぞれの分類を、前記成立する判定規則の項目が多いほど高いランクとなるように複数のランクにランク付けを行い、
少なくとも前記ランク付けによって最も高いランクにランク付けされた分類の電子メールについて、前記所定のメール処理を実行すること、

を特徴とする電子メール処理方法。

【請求項 26】

請求項 25 に記載の電子メール処理方法において、さらに、
前記ランク付けによって最も高いランクにランク付けされた分類以外の分類のうち、少なくともいずれか 1 つのランクの分類について、前記蓄積条件を変更し、前記電子メール処理方法に記載の一連の処理をさらに続行すること、を特徴とする電子メール処理方法。

【請求項 27】

利用者にとって好ましくない所定の種類の電子メールを選び出して処理するためのシステムであって、
電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、受信した前記電子メールを分類して蓄積するメール分類システムと、
前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定する判定システムと、
前記判定の結果に基づいて処理を行う電子メール処理システムと、
を備えることを特徴とするシステム。

【請求項 28】

利用者にとって好ましくない所定の種類の電子メールを選び出して処理するためのサーバ装置であって、
電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、受信した前記電子メールを分類して蓄積するメール分類部と、
前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定する判定部と、
前記判定の結果に基づいて処理を行う電子メール処理部と、
を備えることを特徴とするサーバ装置。

【請求項 29】

コンピュータに、
電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、

受信した前記電子メールを分類して蓄積しする分類機能と、
前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定する判定機能と、
前記判定の結果に基づいて処理を行う電子メール処理機能と、を実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

技術分野

本発明は、電子メールシステムに関し、詳細には、利用者にとって好ましくない電子メールについての処理に関する。

背景技術

従来、携帯電話等のキャリアが提供する電子メールサービスでは、インターネットメールアドレスとして、アカウント名に契約者の電話番号（例えば、09011112222等）を用い、かつ、キャリア共通のドメイン名を用いたものをデフォルトで契約者に割り当てている。このため、ソフトウェアを用いて電話番号の部分をシーケンシャルにまたはアランダムに変更して宛先アドレスを自動的に生成し、これらを用いて不特定多数の契約者に対して広告等のメッセージを送信する業者等が現れた。このために、契約者に対して見知らぬ業者等からの電子メールが何度も届くという事態が発生している。

このような電子メールは、利用者が迷惑と感じる種類のものである。このよう種類の電子メールには、いわゆる spam メールや、UCE (Unsolicited Commercial Email)、UBE (Unsolicited Bulk Email) などと呼ばれる一方的に利用者に送り付けられる電子メールが含まれる。このような利用者が迷惑と感じる電子メールのことを、本明細書では、以下、「好ましくない電子メール」と呼ぶことにする。

キャリアが電子メール受信に対して課金を行う場合、好ましくない電子メールを受信する場合にも契約者は料金を支払わなければならない。また、携帯電話等での電子メールサービスでは、電子メールは携帯電話等に対して逐次配信されるのが一般的であり、契約者は見知らぬ業者からの電子メールが配信されるたびにメ

ール着信の通知を受けることになり、極めて煩雑である。

このような好ましくない電子メールへの対策として、契約者が着信を拒否するアドレスやドメイン名を登録し、これらに該当する発信元からの電子メールの配信をブロックすることが行われている。しかし、契約者が携帯電話端末等を利用して着信拒否アドレスやドメイン名を登録しない限り、好ましくない電子メールの配信を停止することができない。このため、契約者は好ましくない電子メールが届き始める度にこれを登録しなければならず、極めて煩雑である。

特開2000-163341号公報には、電子メール利用者（複数の場合はその個々）に対し、電子メールを受信する条件として、同一の電子メール送信者から受け取ることのできる1日当たりの電子メール件数の上限を設けることにより、同一の電子メール送信者から1日に大量の件数の電子メールを受信することを制限することが開示されている。

さらに、同公報には、既知送信者を登録し、これ以外の発信者からの電子メールを受信することを制限することも開示されている。

発明の課題

しかしながら、特開2000-163341号公報が提案する技術は、同一の電子メール利用者に対して大量の電子メールを配信してそのメールボックスをオーバーフローさせること、メールボックスから電子メールを受信するときに長時間かかるようにすること等、嫌がらせ目的のいわゆるspamメールを排除するための技術である。上述の好ましくない電子メールは特定の利用者に対してはほんの僅かな数、例えば1日当たり1通しか届かないことがあるので、同公報の技術では上述の好ましくない電子メールの対策とはなり得ない。

また、好ましくない電子メールの容量は必ずしも大容量ではない。しかしながら、好ましくない電子メールは何千何万オーダーの契約者に対して1度に配信されるので、特定の契約者に対しては1通の小さなメールであっても、トラフィックの増大、メールサーバへの負荷増大等、電子メールサービス全体に与える影響は図り知れない。

また、メールサーバにおいて、利用者が既知送信者以外からの電子メール受信を制限した場合、利用者が既知送信者の登録を忘れると、例え重要なメッセージを

含む電子メールであっても着信できないことになるので極めて不便である。

本発明は、かかる点に鑑みてなされたものであり、利用者に負担や不便をかけることなく、サービス側で好ましくない電子メールを判定し、適切な対応を行うことが可能な好ましくない電子メールの判定方法、電子メール処理方法およびシステム、および、サーバ装置を提供することを目的とする。

発明の開示

本発明の側面によれば、利用者にとって好ましくない所定の種類の電子メールを選び出して処理するための方法であって、発信元から利用者に至るまでの経路の途中で電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、受信した前記電子メールを分類して蓄積し、前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定すること、を特徴とする電子メール処理方法が提供される。

所定の情報に基づく分類を行った上で、分類毎に所定のアルゴリズムによる判定が行われるので、利用者にとって好ましくない電子メールを確実に判定することができる。

前記所定の情報は、同一の発信元から送信された蓋然性の高い電子メールの一群を特定するための情報であっても良い。

前記同一の発信元から送信された蓋然性の高い電子メールの一群を特定するための情報は、前記電子メールの中継に関する情報であっても良い。

前記中継に関する情報は、中継経路の情報であり、前記分類は該中継経路毎に行われるものであっても良い。

或いは、前記中継に関する情報は、中継経路中にある中継機のサーバ名またはドメイン名であり、前記分類は、該サーバ名またはドメイン名毎に行われるものであっても良い。

前記所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定することは、前記所定の種類の電子メールであるか否かについてランク付けすることを含んでいても良い。

前記電子メール処理方法は、前記ランク付けによるランクに応じて、前記各分類

の電子メールに対して異なる処理を実行することを含んでいても良い。

前記電子メール処理方法は、前記所定のアルゴリズムによって、前記各分類の電子メールを、前記所定の種類の電子メールであるもの、前記所定の種類の電子メールの可能性のあるもの、通常の電子メールの少なくとも3つのランクにランク付けしても良い。

前記ランク付けの段階数は可変であっても良い。

前記所定のアルゴリズムは、前記各分類の電子メールに対して前記ランク付けを行うための基準として用いる、それぞれのランクに対応したしきい値を含むと共に、該しきい値の値は可変であっても良い。

前記所定のアルゴリズムが変更可能であっても良い。

前記電子メール処理方法は、前記所定のアルゴリズムが、前記分類して蓄積された電子メールに関して、それぞれの分類毎に、下記項目、

- (1) 単位時間当たりの受信数が第1所定値以上である
- (2) 宛先アドレスが有効でないメール数が第2所定値以上である

のうち1つ以上を含む判定規則について前記判定規則の各項目が成立するか否かを判定することを含み、

前記判定の結果に基づいて前記各分類の電子メールが前記所定の種類の電子メールであるか否かを判定するものであっても良い。

好ましくない電子メールは、送信先のメールサーバに対して、同一の中継経路をたどって、或いは同一の発信元から一度に大量に送信されてくる場合が多いので、このように送信先のメールサーバに送信される電子メール、或いは送信先から送り返される不達メール等の電子メールを受信して分類し、判定規則を用いて判定を行うことで確実に迷惑メールであることを判定することができる。

前記電子メール処理方法は、前記所定のアルゴリズムが、前記分類して蓄積された電子メールに関して、それぞれの分類毎に、下記の判定規則、

- (1) 単位時間当たりの受信数が第1所定値以上である
- (2) 宛先アドレスが有効でないメール数が第2所定値以上である
- (3) 発信元アドレスが無効である
- (4) 分類内の電子メールの宛先アドレスの相違の度合いが第3所定値以上であ

る

(5) メール本文中に所定の内容が含まれる

(6) メール本文中に所定のURLが含まれる

のうち少なくとも1つについて成立するか否かを判定することを含み、前記判定の結果に基づいて前記各分類の電子メールが前記所定の種類の電子メールであるか否かを判定するものであっても良い。

前記判定規則(4)の宛先アドレスの相違の度合いは、各宛先アドレスの符号の間のハミング距離に基づいて算出されても良い。

前記電子メール処理方法は、前記電子メールを受信して分類し蓄積することを、蓄積時間、蓄積メール数の少なくとも一方を定めた蓄積条件に達するまで行うことを含んでいても良い。

前記電子メール処理方法は、前記判定の結果、前記所定の種類の電子メールと判定された電子メールについて、該判定された電子メールの送信先の利用者の情報が前記所定の種類の電子メールの発信元に送信されることを防止する処理を行うことを含んでいても良い。

前記電子メール処理方法は、前記判定の結果、前記所定の種類の電子メールと判定された電子メールについて、

(a) 利用者への配信をブロックする

(b) 発信元へ、不達の場合にメールサーバが発信元に対して送り返す不達メールを擬似的に再現した疑似エラーメッセージを送信する

(c) 消去する

(d) 所定のメールサーバから不達メールが発信される場合に、当該不達メールが発信元に返信されるのを抑止する

(e) 発信元に対して警告メッセージを送信する

(f) 当該分類の電子メールに関する情報を保存しておく

(g) 利用者に対し当該分類の電子メールを配信すべきか否かの問い合わせを行い、該問い合わせに対する利用者からの応答に応じて処理を行う

(h) 当該分類の発信元に対応する装置に対しては、所定のメールサーバについてのドメインネームサービスが拒否されるようにする

(i) 当該分類の発信元に対応する装置のIPアドレスに対しては、所定のメールサーバに対する接続の要求が拒否されるようにする

のうち少なくとも1つを含む処理を行うことを含んでも良い。

この場合、好ましくない電子メールと判定し得る分類の電子メールについては、配信ブロック等により利用者に迷惑がかからないようにすることが可能である。前記電子メールは、送信先の利用者への電子メールが不達であった場合に、所定のメールサーバから発信元に転送される不達メールを含んでも良い。

本発明の別の側面によって提供される電子メール処理方法は、電子メールを受信すると共に、該受信した電子メールに含まれる発信元および／またはメールの中継に関する情報に基づいて、前記受信した電子メールを分類して蓄積し、前記電子メールを受信して分類し蓄積することを、蓄積時間、蓄積メール数の少なくとも一方を定めた蓄積条件に達するまで行う。そして、下記の項目(1)から(6)

、

- (1) 単位時間当たりの受信数が第1所定値以上である
- (2) 宛先アドレスが有効でないメール数が第2所定値以上である
- (3) 発信元アドレスが無効である
- (4) 分類内の電子メールの宛先アドレスの相違の度合いが第3所定値以上である
- (5) メール本文中に所定の内容が含まれる
- (6) メール本文中に所定のURLが含まれる

のうち1つ以上を含む判定規則に関して前記判定規則に含まれる項目のうちどの項目を適用するかを指定した判定規則適用条件に基づいて、前記分類して蓄積された電子メールについて、前記それぞれの分類毎に、前記判定規則適用条件で指定された各項目が成立するか否かを判定する。したがって、各分類毎に、判定規則の各項目のうち成立している項目数が得られ、好ましくない電子メールであるかどうかを、成立した判定規則の項目数に基づいて決定することが可能になる。さらに、前記判定規則適用条件で指定された項目のうち、成立する項目の数を判定成立の条件として用いる総合判定規則にしたがって、前記それぞれの分類毎に、前記総合判定規則が成立するかどうかの判定を行い、前記総合判定規則が成立

すると判定された分類の電子メールについて、

(a) 利用者への配信をブロックする

(b) 発信元へ、不達の場合にメールサーバが発信元に対して送り返す不達メールを擬似的に再現した疑似エラーメッセージを送信する

のうち少なくとも1つを含む所定のメール処理を実行する。したがって、迷惑メールと判定し得る分類の電子メールについては、配信ブロック等により利用者に迷惑がかからないようにすることが可能である。

前記電子メール処理方法は、さらに、前記電子メール処理方法に記載の一連の処理を少なくとも1回以上実行することによって、前記総合判定規則の判定結果に関する統計的な値を取得し、取得された前記統計的な値に応じて、前記蓄積条件、前記判定規則、前記判定規則適用条件、前記総合判定規則のうち少なくともいずれか1つについて内容の設定または変更を行うことを特徴としても良い。例えば、全受信メール数のうち総合判定によって迷惑メールと判定される電子メール数の割合が、一般の利用者の感覚に促した値となるように、上記各規則、条件等を変更することができる。

前記電子メール処理方法は、さらに、前記蓄積条件、前記判定規則、前記判定規則適用条件、前記総合判定規則のうち少なくともいずれか1つについて、ユーザインタフェースを介して内容の設定または変更を受け付けることを特徴としても良い。

前記電子メール処理方法は、さらに、前記総合判定規則が成立した場合でも、所定の例外規則に該当する分類については前記所定のメール処理の対象とはしないことを特徴としても良い。

前記所定の例外規則は、例外とすべき発信元のアドレス、例外とすべき発信元のドメイン名、前記所定のメール処理を実行しない時間帯、前記所定のメール処理を実行しない期間の少なくともいずれか一つを含むものであっても良い。

電子メール処理方法は、さらに、利用者が所定のメールサーバに対して、ドメイン名、発信元アドレスの少なくとも1つを含む、電子メールの配信を希望しない配信拒否条件の登録をしている場合に、前記所定のメールサーバから前記配信拒否条件を取得し、取得した前記配信拒否条件に基づいて前記所定のメール処理の

対象とする分類を決定することを特徴としていても良い。したがって、配信されたメールに対する利用者の挙動を反映することができる。

電子メール処理方法は、前記総合判定規則に前記判定規則適用条件で指定された判定規則の項目のうち、成立する判定規則の項目の数がランク付けの要因として定められ、総合判定規則にしたがって、前記それぞれの分類を、前記成立する判定規則の項目が多いほど高いランクとなるように複数のランクにランク付けを行い、少なくとも前記ランク付けによって最も高いランクにランク付けされた分類の電子メールについて、前記所定のメール処理を実行することを特徴としていても良い。

電子メール処理方法は、さらに、前記ランク付けによって最も高いランクにランク付けされた分類以外の分類のうち、少なくともいずれか1つのランクの分類について、前記蓄積条件を変更し、前記電子メール処理方法に記載の一連の処理をさらに続行することを特徴としていても良い。例えば、蓄積条件をより厳しい条件に変更して観察を続行することで、迷惑メールをいっそう効果的に見つけ出すことが可能になる。

本発明の別の側面によれば、利用者にとって好ましくない所定の種類の電子メールを選び出して処理するためのシステムであって、電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、受信した前記電子メールを分類して蓄積するメール分類システムと、前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定する判定システムと、前記判定の結果に基づいて処理を行う電子メール処理システムと、を備えることを特徴とするシステムが提供される。

本発明の別の側面によれば、利用者にとって好ましくない所定の種類の電子メールを選び出して処理するためのサーバ装置であって、電子メールを受信し、該受信した電子メールに含まれる所定の情報に基づいて、受信した前記電子メールを分類して蓄積するメール分類部と、前記分類して蓄積された電子メールについて、前記分類毎に、所定のアルゴリズムにしたがって前記所定の種類の電子メールであるか否かを判定する判定部と、前記判定の結果に基づいて処理を行う電子

メール処理部と、を備えることを特徴とするサーバー装置が提供される。

発明の実施の形態

以下、本発明の実施の形態について図面を参照して説明する。

以下、本発明の実施形態に関する説明では、「好ましくない電子メール」を選び出して処理する機能を持つメール処理サーバ51を、通常のメールサーバ61とインターネット30の間に配置して構成したメール処理システムに関して説明する。すなわち、図1に示すように、メール処理サーバ51は、ゲートウェイ41とメールサーバ61の間に配置され、メールサーバ61に対して送信される電子メールのうち、好ましくない電子メールがあるかどうかを判定するように構成されている。メール処理サーバ51は、例えば、好ましくない電子メールであると判定した電子メールがメールサーバ61に配信されることをブロックすることができる。

図1を参照して、電子メールが、発信元端末11からメールサーバ61の利用者側の端末である移動体端末81に送信される際の動作について説明する。なお、図1において、発信元端末11は、インターネット30に接続されている。したがって、発信元から送信先の移動体端末81への電子メールは、例えば、インターネット標準のTCP/IPプロトコル上で動作するアプリケーションである、SMTP (Simple Mail Transfer Protocol) プロトコルにしたがって、送信元メールサーバ13からメールサーバ61まで転送される。メールサーバ61から移動体端末81へのメール配信形態は、通知だけをプッシュするもの、メール内容を全てプッシュするものなど、様々な形態がある。本発明の実施形態において、これらの様々な配信形態をとることができる。発信元端末11からの電子メールが、いま、図1の矢印に示すような中継経路に沿って配信されたものとする。すなわち、発信元端末11からの電子メールは、送信元メールサーバ13、中継機A、B、CおよびDを介して、インターネットと携帯電話網を仲介するゲートウェイ41まで転送される。さらに、この電子メールは、ゲートウェイ41から、メール処理サーバ51、メールサーバ61、および基地局71を介して利用者の移動体端末81に配信される。中継機A、B、C、Dは、最終宛先へメールを転送するのに適切な次の中継機へメールを転送す

る。また、中継機A-Dのドメイン名が、それぞれドメインA-Dであるものとする。ここで留意すべきことは、以上のようにインターネットを介して、電子メールが同一の発信元から同一の利用者に向けて送信される場合、その中継経路は同一であるとみなすことができるということである。特に、短い時間に極めて大量のメールが送信される場合、その確率はさらに高くなる。

電子メールは、メッセージヘッダとメッセージ本体で構成される。したがって、メール処理サーバ51において、メールサーバ61に向けて配信される電子メールを受信しそのメッセージヘッダを解析することで、その中継経路（図1の例でいえば、中継経路が中継機A→B→C→Dであること）を知ることができる。メッセージヘッダに含まれるフィールドの例を以下に示す。

- ・ From : (発信者のアドレス)
- ・ To : (宛先のアドレス)
- ・ Received : (途中で中継した中継機名)
- ・ Subject : (メッセージの題名)

図2は、メール処理サーバによって実行される、好ましくない電子メールの処理についてのフローを示す図である。図2に示す処理の流れに沿って、メール処理サーバ51の動作の詳細を説明する。

初めにステップS001において、ゲートウェイ41からメールサーバ61に送信される電子メールをネットワークから受信する。

そして、受信した電子メールのヘッダメッセージを解析し（S002）、所定の分類ルールにしたがって分類を行う（S003）。ステップS003において用いることのできる分類ルールとして、以下のものを適用可能であるものとする。

- b1. 中継経路
- b2. 中継機（サーバ名、ドメイン名）
- b3. 発信元（ドメイン名、アドレス）
- b4. 本文中のキーワード

「b1. 中継経路」は、中継機の中継順序についての情報であり、図1の例でいえば、中継経路は中継機A→B→C→Dである。つまり、分類ルールとして上記「b1. 中継経路」を用いると、中継経路ごとに電子メールを分類することがで

きる。上述のように、電子メールが同一の発信元からメールサーバ61に送信されるときの中継経路は、同一であるとみなすことができる。したがって、この「b1. 中継経路」によってメールを分類することは、好ましくない電子メールの発信元を見つけ出す手段として極めて有効であることに注目する必要がある。

上記「b2. 中継機」は、中継機のサーバ名またはドメイン名によって分類を行うためのルールである。上記「b3. 発信元」は、発信元のドメイン名またはアドレスによって分類を行うためのルールである。また、上記「b4. 本文中のキーワード」は、本文中のキーワードに基づいて分類を行うためのルールである。ここで、「b1. 中継経路」、「b2. 中継機」とは、ヘッダメッセージに含まれる、メールの中継に関する情報と位置づけることができ、また、「b3. 発信元」は、ヘッダメッセージに含まれる、発信元に関する情報と位置づけることができる。また、「b4. 本文中のキーワード」についても、例えばURLのように、発信元に関する情報として用いることができるものがある。

ここでは、分類ルールとして「b1. 中継経路」を用いるものとして以下の説明を行う。さらに、ステップS003において、分類ルールにしたがって分類した電子メールを、蓄積条件C11（蓄積するメール数または蓄積時間）にしたがって蓄積する。つまり、蓄積条件が成立するまで、メール受信S001、メール解析S002、分類・蓄積S003の一連の処理を繰り返す。

蓄積条件が成立するまでメールの分類・蓄積が行われると、次に、判定ルール適用条件C21が読み出され（S004）、読み出された判定ルール適用条件にしたがって、分類毎に、判定ルール個々が成立するかどうかの判定が行われる（S005）。なお、ここではまだ、各分類の電子メールが好ましくない電子メールであるかどうかの総合判定は行われない。判定ルール適用条件C21とは、適用可能な判定ルール（例えば、下記j1.～j6.）のうち、どの判定ルールを用いるかを定義したものである。

- j1. 単位時間あたりの受信メール数が第1所定値以上である
- j2. 単位時間当たりの不達メール数が第2所定値以上である（不達であるかは宛先アドレスが有効であるか否かで判断する）
- j3. 発信アドレスが無効である

j 4. 宛先アドレスの符号間のハミング距離に基づいて求めた、時間的に連続するメールのアドレスが相違する度合いが第3所定値以上である

j 5. メール本文に所定の内容が含まれる

j 6. メール本文に所定のURLが含まれる

上記判定ルールj 1～j 6について説明する。

判定ルール「j 1. 単位時間あたりの受信メール数が第1所定値以上である」とは、1つの分類に蓄積された電子メールについて、単位時間当たりの受信数を計算し、計算結果の受信数が第1所定値以上であるか否かを判定することを表している。上述のように、好ましくない電子メールは、同一の中継経路をたどって短時間に膨大な量が送信されるので、この判定ルールを用いることによって、1つの分類に属する電子メールが好ましくない電子メールであることを極めて効果的に判定することが可能である。

判定ルール「j 2. 単位時間当たりの不達メール数が第2所定値以上である」とは、1つの分類に蓄積された電子メールのうちの不達メール、すなわち、宛先アドレスが有効な宛先アドレスとなっていないものをカウントし、この不達メールの単位時間あたりの受信数が第2所定値以上であるか否かを判定することを表している。上述のように、好ましくない電子メールは、宛先アドレスを、コンピュータ上でシーケンシャルに、或いはアランダムに自動的に発生させることによって生成されていることがある。したがって、このような好ましくない電子メールが蓄積されていると、分類内のメールのうち、不達メール（宛先アドレスが有効でないものとしてカウントされるもの）が多くなる。したがって、判定ルールj 2. によって、好ましくない電子メールであるか否かを判定することができる。

判定ルール「j 3. 発信アドレスが無効である」とは、蓄積されたメールのヘッダメッセージにおいて発信アドレスが記述されていない場合を含み、発信アドレスが無効であるかどうかを判定することを表している。好ましくない電子メールの発信者は、発信アドレスを分からなくするために、ヘッダメッセージ中に発信アドレスが含まれないようにして、或いは発信アドレスを無効なものにしてメール送信することがある。したがって、判定ルールj 3. によって、好ましくない電子メールであるか否かを判定することができる。

判定ルール「j 4. 宛先アドレスの符号間のハミング距離に基づいて求めた、時間的に連続するメールのアドレスが相違する度合いが第3所定値以上である」とは、蓄積されたメールの宛先アドレスの相違の度合いを判定することを表している。一度に膨大な量の相手に電子メールを送りつける好ましくない電子メールの場合、宛先アドレスの相違の度合いが大きくなるので、好ましくない電子メールは、蓄積された電子メールの宛先アドレスの符号間のハミング距離が大きくなることによって特徴づけられる。したがって、判定ルールj 4. によって、好ましくない電子メールであるか否かを判定することができる。

判定ルール「j 5. メール本文に所定の内容が含まれる」とは、メール本文中に好ましくない電子メールに相当するような表現がふくまれているか否かを判定するものである。また、判定ルール「j 6. メール本文に所定のURLが含まれる」は、メール本文中に、好ましくない電子メールに相当するURLが含まれているか否かを判定するものである。

判定ルール適用条件C 2 1は、以上の判定ルールj 1. ~ j. 6のうちどれを適用するかを定義したものである。なお、判定ルール適用条件C 2 1には、上記第1所定値、第2所定値および第3所定値としてどのような値を用いるかが含まれていても良い。

図2に戻りステップS 0 0 6では、総合判定規則C 3 1が読み出され、次に、それぞれの分類について好ましくない電子メールであるかどうかの総合判定が行われる(S 0 0 7)。ここで、総合判定規則C 3 1とは、判定ルール適用条件C 2 1による判定結果と、総合判定(ランク0、ランク1、ランク2)とを対応づけたものである。すなわち、総合判定規則C 3 1を用い、個々の判定ルールの判定結果に応じて、利用者にとっての迷惑の度合いを、ランク0、ランク1、およびランク2の3つにランク付けする。

なお、総合判定S 0 0 7において、正規事業者等からの電子メールが好ましくない電子メールとされることがないように、正規事業者等に関する例外ルールC 5 1が適用される。例外ルールC 5 1には、例えば、正規広告事業者などの正規事業者のアドレスやドメイン、大学等の合格通知案内に使用されるアドレスやドメインなどを含めることができる。さらに、例外ルールとして、配信を特別に許可

する時間帯や期間（日、週、月）等を含めても良い。

総合判定S007が行われると、次に、判定結果が記録される（S008）。総合判定は、総合判定規則C31に基づいて行われる。下記表1に総合判定規則C31の一例を示す。表1では、個別の判定ルールのうち成立するものが所定数X未満であることにより、好ましくない電子メールではないと判定できるものを「ランク0」としている。また、例えば、個別の判定ルールのうち成立するものが所定数X以上Y未満（但し、 $Y > X$ ）であることにより、好ましくない電子メールの可能性があると判定できるものを「ランク1」としている。また、例えば、個別の判定ルールのうち成立するものの数がY以上であることにより、好ましくない電子メールと判定できるものを「ランク2」としている。

表 1

成立した判定ルールの数	ランク
成立した判定ルールの数 $\geq Y$	ランク 2
$Y > \text{成立した判定ルールの数} \geq X$	ランク 1
$X > \text{成立した判定ルールの数}$	ランク 0

「ランク0」と判定された分類については、好ましくない電子メールではないので、メールサーバ61に対して配信処理をする（S012）。「ランク0」と判定された分類については、配信した後廃棄することができる。一方、「ランク1」と判定された分類については、メールサーバ61への配信処理を行った後（S013）、その分類を残したまま引き続き観察継続（S015）を行う。すなわち、「ランク1」の分類を残したまま、蓄積条件、判定ルール、判定ルール適用条件を、例えばより厳しい条件となるように変更して、S001からの処理を続行する。このような構成にすることで、好ましくない電子メールを確実につきとめることができる。

なお、総合判定結果が「ランク0」、「ランク1」であった場合に、利用者の挙動を観察して（S017）、その結果を蓄積条件、判定ルール、判定ルール適用条件に反映させても良い。すなわち、メールサーバ61が持つ、配信拒否条件登録部と連携し、配信したメールに対するユーザ挙動を観察する。ユーザ挙動の観察とは、例えば、発信元アドレスまたはドメイン名について、利用者がメールサーバ61に配信拒否登録をしたかどうかを観察することである。例えば、「ラン

ク0」と総合判定してメール配信を行ったにも拘わらず複数の利用者が配信拒否の登録を行った場合に、蓄積条件、判定ルール、判定ルール適用条件をいっそう厳しい条件となるように変更することができる。なお、ユーザ挙動の観察に、利用者が、配信されたメールに対する返信を行ったか否かを加えても良い。挙動観察(S017)を行った後、メール受信(S001)からの処理を続行しても良い。

或いは、ユーザ挙動の統計をとっておき、所定条件が成立したら迷惑メールであるとみなして、当該分類の中継経路などを介して送信されてくるメールを以後迷惑メールとして処理しても良い。例えば、利用者に対しメール配信を行ってから、利用者の50%が迷惑メールであることに気が付く時間Tを例えば28800秒とし、その段階で配信拒否条件の登録をする利用者が、全利用者のn%（例えば3%）を超えたら迷惑メールであるものとして処理しても良い。

「ランク2」と判定された分類の電子メールに対しては、以下で説明する所定のメール処理を行う(S014)。なお、「ランク2」と判定された分類、すなわち、「ランク2」と判定された中継経路をたどって送信されてくる電子メールについては、その後受信されるものについても所定のメール処理を行うことができる。メール処理サーバ51は、所定のメール処理として、(1)配信ブロック、(2)疑似エラー送信、(3)消去、(4)不達メール抑止、(5)警告、(6)証拠収集、(7)確認後送信等を行うことができる。

「(1)配信ブロック」とは、「ランク2」の分類の電子メールについてはメールサーバ61に配信を行わない、すなわち、利用者に届かないようにすることである。

「(2)疑似エラー送信」とは、好ましくない電子メールであると判定された分類の電子メールの発信元へ、本来不達の場合にメールサーバが発信元に対して送り返す不達メールを擬似的に再現した疑似エラーメッセージを送信することである。好ましくない電子メールの発信元は、送信先から不達メールが返ってきたかどうかによって、自信が保有する宛先アドレスのデータベースの有効性を高めていることがある。疑似エラーを返すことで、好ましくない電子メールの発信元がこのようなデータベースを維持するメリットをなくし、好ましくない電子メール

による利用者への迷惑度を低減することができる。

「(3) 消去」とは、「ランク2」と判定された分類に蓄積されたメールを消去してしまうことである。

「(4) 不達メール抑止」とは、原則的に利用者へメール配信を行うことを前提とする処理であり、宛先アドレスが有効でないことなどにより、メールサーバ61から発信元に対して不達メールが発信される場合に、その不達メールを受信して抹消し、不達メールが発信元に返信されるのを抑止することである。このことによって、不達メールの発信元において、不達メールのヘッダメッセージの内容（中継経路等）が解析されること等を防ぐことができる。

「(5) 警告」とは、好ましくない電子メールの発信元に対して警告メッセージを送信することである。

「(6) 証拠収集」とは、好ましくない電子メールそのもの、または好ましくない電子メールに関する情報を記録しておくことである。この「(6) 証拠収集」は、「(1) 配信ブロック」を行うことなく行うことが好ましい。後に、好ましくない電子メールがあったことの証明とすることができる。

「(7) 確認後送信、」とは、「ランク2」と判定されたメールをどのように扱うかについて、利用者に問い合わせた上で処置することである。例えば、「ランク2」と判定されたメールのヘッダメッセージの内容のみ利用者に送り、利用者が配信を許可した場合にのみ配信するようにする。

以上で述べたことから理解されるように、メール処理サーバ51は、所定のメール処理として、宛先アドレスの利用者がいるか否かに応じて、下記表2に示すように、一般的なメールサーバとは異なる処理を選択的に実現することができる。

表 2

利用者	動作
いる	発信元に対しては、ユーザがいないふりをする（例えば、疑似エラーを返す）
いる	発信元に一切の送信を行うことなく、蓄積したメールを消去する
いない	発信元に不達メールが返信されることを抑止する

ここで説明した、好ましくない電子メールに対する所定のメール処理は、単独で

実行しても良いし適宜併用することもできることが理解できる。また、上記の所定のメール処理は例示であって、上記内容の変形や、上記の例とは異なる様々なメール処理を追加として行うことが可能である。

例えば、メールサーバ61のドメインを管轄するドメインネームサーバと連携することにより、好ましくない電子メールの送信元メールサーバ13が、送信先のメールサーバ61のアドレスを取得できないように、DNS（ドメインネームサービス）を拒否する構成とすることもできる。

また、発信元（発信元端末、送信元メールサーバなど）のIPアドレスからの接続をメール処理サーバ51などで拒否することによって、IP接続ができないようにすることも可能である。なお、ステップS014のメール処理が終了したら、メール受信（S001）からの処理を続行しても良い。

図3は、総合判定規則C31と、判定ルール適用条件C21に対する更新処理を示している（ステップS030）。この更新処理は、ユーザインタフェースを介してメール処理サーバ51の管理者などが行える構成で当であっても良い。或いは、この更新処理は、総合判定結果に関する統計に基づいて自動的に更新を行う構成であっても良い。例えば、総合判定結果に関する統計として、「ランク2」と判定される電子メール数が、全受信メール数に占める割合を求める。そして、この割合が所定の割合となるように、総合判定規則C31、判定ルール適用条件C21等を変化させても良い。この場合、好ましくない電子メールの判定を、現実の発生状況に応じて、すなわち、「迷惑」と感じる利用者の感覚、社会情勢などに対応して柔軟に変化させることが可能になる。なお、この更新処理（S030）において、蓄積条件C11と例外ルールC51がさらに更新できる構成であっても良い。

図4は、メール処理サーバ51として用いることができるサーバ装置の一般的な構成を示している。図4に示すように、メール処理サーバ51は、CPU101にRAM105、ROM193、ディスク装置107、およびネットワークインタフェース113などが接続されて構成される。ネットワークインタフェース113を介してネットワークに接続された他の装置との通信が行われる。図2、図3に示す電子メールに関する処理を実現するプログラムは、ディスク装置107

に格納され、CPU 101がこのプログラムを読み出して実行する。

上述の本発明の実施形態は、様々な特徴を持つものとして記載されてきたが、適宜、上述の特徴の省略、変形、置換をすることによって、実施形態の様々な変形例を構成することができる。例えば、上述の実施形態において、メール処理サーバ51は、メールサーバ61とゲートウェイ41の間にある専用のサーバとして構成されているが、メール処理サーバ51の機能を、メールサーバ61などの他のサーバに統合した構成にすることも可能である。或いは、図2に示した各処理を複数のサーバ装置で分担して行う構成も可能である。

なお、メール処理サーバ51が担う図2、図3のような機能を、例えばより小型の専用の装置に実現することも可能である。

また、本発明は、プッシュ型のメール配信の場合のみだけでなく、プル型のメール配信の場合にも適用できることはいうまでもない。

図2で示した、メールの蓄積から所定のメール処理等に至る一連の処理は、上述の実施形態で述べたように繰り返し常時行う構成以外にも、定期的にまたは管理者によって任意のタイミングで行う構成とすることも可能である。配信ブロックは原則的に行わないこととし、メールを蓄積する場合（図2のS003）において、メールそのものを蓄積するのではなく、メールの一部または全部をコピーしたデータについて、好ましくない電子メールであるか否かを定期的（毎日または毎月）に判定する構成とすることも可能である。

上述の実施形態では、上記の分類毎に同一の判定ルール適用条件を適用しているが、判定ルール適用条件を、上記の分類毎のみだけでなく、送信元メールサーバ毎、利用者毎など、より詳細な項目毎に適用する構成とすることも可能である。なお、上述した実施形態は、発信元から送信先のメールサーバに送信されるメールを受信して、分類、蓄積および判定を行う構成である。同様に、送信先のメールサーバから発信元へ送信される不達メールを受信して、分類、蓄積および判定を行った場合にも、好ましくない電子メールであるか否かの判定を行うことが可能である。

上述した判定ルール（j1. ～ j6.）の変形例も有り得る。例えば、判定ルールj2.等は、単位時間当たりの不達メール数というような絶対的な基準となっ

ている。しかしながら、このような絶対的な基準に代えて、分類内の全受信メールのうち何%が不達メールとなっているかというような、相対的な基準を用いることも可能である。

総合判定S007に関する様々な変形例も有り得る。例えば、上述の実施形態では、「ランク2」、「ランク1」、「ランク0」の3つのランクで総合判定を行っているが、ランク付けの数をさらに増やしても良いし、また、「ランク2」、「ランク0」の2ランクの判定としても良い。総合判定S007では、判定ルール(j1.～j6.)の成立数によってランク付けを行っているが、いずれかの判定ルールに重み付けを行っても良い。

上述したように、好ましくない電子メールは、同一の発信元から一度に大量に発信されるという性質があり、また、好ましくない電子メールの発信者は、ヘッダメッセージ中の発信者のアドレスが分からないようにして送信する場合もある。この意味において、中継経路の情報(上記分類ルールb1. 中継経路)は、同一の発信元から送信された蓋然性の高い電子メールの一群を特定する分類ルールの一つとして極めて有効である。上記の「中継経路A→B→C→D」のような中継経路の情報に限らず、中継経路の情報の一部、或いは中継機の情報(上記分類ルールb2. 中継機のサーバ名、ドメイン名)のような、メールの中継に関する他の情報も、同一の発信元から送信された蓋然性の高い電子メールの一群を特定する分類ルールとして有効であることは明らかである。発信元の情報(上記分類ルールb3. 発信元のドメイン名、アドレス)がヘッダメッセージ中に含まれるならば、発信元の情報进行分类ルールとして用いることが有効であることは当然である。

発信元やメールの中継に関する情報以外にも、メールの標題、本文中のキーワード、添付ファイルの内容など、メールに含まれる様々な情報を、同一の発信元から送信された蓋然性の高い電子メールの一群を特定する分類ルールとして用いることができる。例えば、メール本文中に含まるURLのような発信元に関する情報を用いて分類することによって、同一の発信元から送信された蓋然性の高い電子メールの一群を特定することができる。メール中の特定の表現によって、発信元を特定可能な場合もある。

或いは、発信元アドレス等の特定の情報がヘッダメッセージ中に記載されていない場合には、発信元アドレスが秘匿されている旨の情報として利用することができる。メールに含まれる情報としての、発信元アドレスが秘匿されている旨の情報も、そのような秘匿が特定の好ましくない電子メールの送信者によって行われているならば、同一の発信元から送信された蓋然性の高い電子メールの一群を特定する分類ルールとして用いることが可能である。

このように、同一の発信元から送信された蓋然性の高い電子メールの一群の分類分けを行えば、後は分類毎に、単位時間当たりの受信数が所定値以上であるというような所定のアルゴリズムを用いることによって、分類された一群の電子メールが好ましくない電子メールであることを判定することが可能である。なお、この所定のアルゴリズムとしては、上述の実施形態において例示した判定ルール j 1. ～ j 6. 以外にも、好ましくない電子メールの性質に基づく他のアルゴリズムを適用することができる。判定ルール (j 1. ～ j 6.) は、単独で用いても良いし、組み合わせて用いても良いことは上述の実施形態の通りである。また、判定ルール (j 1. ～ j 6.) に加える形で、他のアルゴリズムを用いても良い。

好ましくない電子メールの発信元がメールアドレスをコンピュータ等によって順次生成しているとすれば、受信アドレスの長さ等によって分類することも可能である。また、好ましくない電子メールの発信者が、同一内容のものを大量配信しているとすれば、メール全体の長さを適当な長さ（例えば、32バイト）に区切ってそれぞれについて分類することも可能になる。

メールに含まれる情報には、同一の発信元から送信された蓋然性の高い電子メールの一群を特定するための情報以外にも、メールの内容の性質から好ましくない電子メールであることを特定できるタイプの情報がある。例えば、好ましくない電子メールの可能性を示す表現等が標題、本文中等に含まれる場合、このような表現を含むメールを分類して蓄積し、上述の所定のアルゴリズムの一つ、例えば、単位時間あたりの受信数が所定値以上であるかどうかということを用いて、好ましくない電子メールであるか否かを判定することも可能である。なお、明らかに好ましくない電子メールと考えられる表現等が標題、本文中などに含まれてい

る場合には、そのメールについて、好ましくない電子メールであると判定して配信ブロック等の所定のメール処理の対象とすることができる。

このように、受信した電子メールを、メール中の所定の情報に基づいて分類して蓄積し、分類毎に所定のアルゴリズムを用いることによって、好ましくない電子メールであるか否かを有効に判定することができる。

なお、以上説明してきた内容において、好ましくない電子メールによる利用者への被害を防止するという観点から、好ましくない電子メールの判定ルールの一部、および所定のメール処理の一部には、メールの消去、メールの開封等の処理が含まれている。これらの処理は、利用者との契約等により合法的な範囲で行うことが好ましく、また、そのように本発明の実施形態を構成できる。

以上説明したように、本発明によれば、サーバー装置等において、好ましくない電子メールを確実に判定し、配信ブロックなどのメール処理の対象とすることができる。好ましくない電子メールによる利用者への被害を効率的に防止することが可能である。好ましくない電子メールの受信を避けるための利用者による介入は一切必要なく、したがって利用者にとって極めて有益である。

なお、上記図2および図3、およびそれに関連して説明された電子メールの処理の機能は、コンピュータ実行可能なプログラムとして、コンピュータにより読み取り可能な記録媒体に格納することができる。なお、コンピュータ上で実行されたときに、以上で説明した電子メールの処理の機能を実現するプログラム、およびこのプログラム記録した記録媒体も本発明の範囲内にある。

なお、以上説明した実施形態は、例示的なものであり、本発明は、上記実施形態の内容により限定されるものではなく、請求の範囲に記載された内容に基づいて理解されるべきものである。

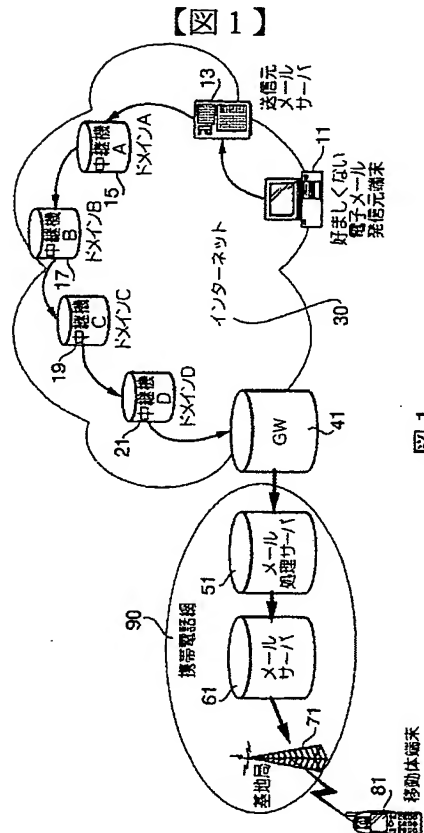
【図面の簡単な説明】

図1は、本発明の実施形態のメール処理サーバによるシステムを表すとともに、発信元からの電子メールの配信経路を表す図である。

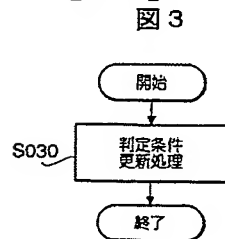
図2は、図1のメール処理サーバにおけるメール処理を表すフローチャートである。

図3は、判定条件の更新処理を表すフローチャートである。

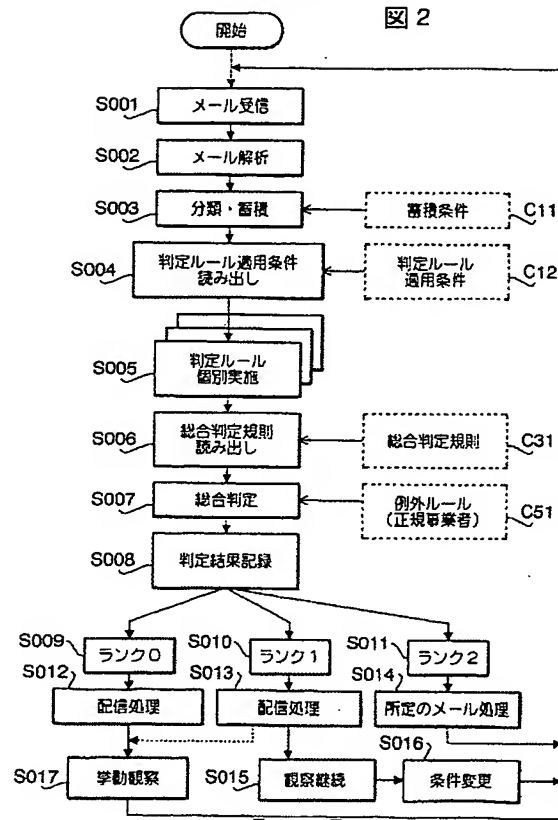
図4は、メール処理サーバの構成を表すブロック図である。



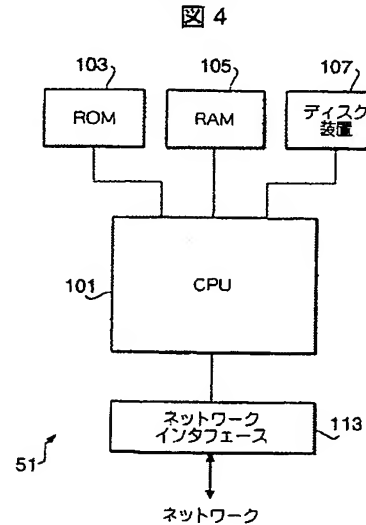
【図3】



【図2】



【図4】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/01831

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁷ H04L12/58, G06F13/00 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int.Cl ⁷ H04L12/58, G06F13/00 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003 Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-353133 A (International Business Machines Corp.), 19 December, 2000 (19.12.00), Full text; all drawings & GB 2350747 A	1-29
A	JP 11-15756 A (Omron Corp.), 22 January, 1999 (22.01.99), Full text; all drawings & US 6199103 B1	1-29
A	JP 10-322384 A (Nippon Telegraph And Telephone Corp.), 04 December, 1998 (04.12.98), Par. Nos. [0012] to [0021] (Family: none)	1-29
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 27 May, 2003 (27.05.03)		Date of mailing of the international search report 10 June, 2003 (10.06.03)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/01831

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-163341 A (NEC Corp.), 16 June, 2000 (16.06.00), Par. Nos. [0007] to [0017] (Family: none)	1-29
A	JP 2001-94591 A (Hitachi, Ltd.), 06 April, 2001 (06.04.01), Par. Nos. [0010] to [0015] (Family: none)	1-29

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

国際調査報告		国際出願番号 PCT/JPO3/01831	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int. Cl ⁷ H04L12/58, G06F13/00			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int. Cl ⁷ H04L12/58, G06F13/00			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1926-1996年 日本国公開実用新案公報 1971-2003年 日本国登録実用新案公報 1994-2003年 日本国実用新案登録公報 1996-2003年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
A	JP 2000-353133 A(インターナショナル・ビジネス・マシーンズ・コーポレーション) 2000.12.19、全文、全図 & GB2350747 A	1-29	
A	JP 11-15756 A(オムロン株式会社) 1999.01.22、全文、全図 & US6199103 B1	1-29	
A	JP 10-322384 A(日本電信電話株式会社) 1998.12.04、段落0012-0021 (ファミリーなし)	1-29	
A	JP 2000-163341 A(日本電気株式会社) 2000.06.16、	1-29	
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願		の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献	
国際調査を完了した日 27.05.03		国際調査報告の発送日 10.06.03	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 江嶋 清仁 電話番号 03-3581-1101 内線 3556	

様式PCT/ISA/210 (第2ページ) (1998年7月)

国際調査報告		国際出願番号 PCT/JPO3/01831
C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	段落0007-0017 (ファミリーなし) JP 2001-94591 A(株式会社日立製作所) 2001.04.06、 段落0010-0015 (ファミリーなし)	1-29

様式PCT/ISA/210 (第2ページの続き) (1998年7月)

フロントページの続き

(注) この公表は、国際事務局 (W I P O) により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願 (日本語実用新案登録出願) の国際公開の効果は、特許法第 1 8 4 条の 1 0 第 1 項 (実用新案法第 4 8 条の 1 3 第 2 項) により生ずるものであり、本掲載とは関係ありません。

THIS PAGE BLANK (CSPC)